УДК 004.942

Г. С. КИРИЧЕНКО, Харківський національний ун-т внутрішніх справ,
О. В.СТРУКОВА, Харківський національний ун-т внутрішніх справ

СТАТИСТИЧНИЙ МЕТОД СТЕГАНОАНАЛІЗУ

В статті розглянуто один із методів стеганоаналізу малюнків, який використовує статистичні критерії. Докладно роз'яснена методика виявлення прихованих вкладень. Подаються практичні результати, одержані з використанням цього методу.

В статье рассмотрен один из методов стеганоанализа рисунков, который использует статистические критерии. Обстоятельно разъясненная методика выявления скрытых вложений. Подаются практические результаты, полученные с использованием этого метода.

One of methods of stegananalysis pictures is considered in the article, which uses statistical criteria. It is detailed the explained method of exposure of the hidden inserts. The practical results got with the use of this method are given.

Стеганографія є способом приховування передачі інформації, розміщуючи її в графічних файлах, відео- та аудіо-файлах тощо. Такою інформацією може бути не злочинна (конфіденційна чи секретна) і в цьому випадку стеганографія використовується як спосіб захисту інформації. Разом із тим стеганографія дозволяє приховувати передачу інформації злочинного характеру, що по суті є порушенням інформаційної безпеки [1].

Засобом виявлення прихованих даних методами стеганографії є стеганоаналіз.

На сьогодні існує декілька методів стеганоаналізу. Один із них полягає в такому .

Більшість методів вбудовування даних у графічні файли якимсь чином змінюють найменш значущі бити LSB (Least Significant Bit). Ідея статистичного стеганоаналізу полягає у порівнянні теоретичного розподілу найменш значущих біт малюнку, в який вбудовані приховані дані, з фактичним розподілом найменш значущих біт у цьому малюнку. При цьому міра схожості теоретичного та фактичного розподілу є мірою вірогідності вбудовування прихованої інформації [2]. Міру схожості можна визначити за допомогою відповідних статистичних критеріїв.

В ідеальному випадку для порівняння теоретичного і фактичного розподілу бітів потрібний оригінал зображення, тобто малюнок без вбудованих даних. Але в більшості випадків оригіналу немає. Тому однією із задач стеганоаналізу є одержання теоретичного розподілу, характерного для стеганограм, тобто розподілу частот, який одержується після вбудовування даних.

Одним із статистичних критеріїв згоди є критерій χ^2 (Пірсона). За допомогою цього критерію встановлюється із заданим рівнем значимості однорідність теоретичного та емпіричного розподілів [3]. За наявними теоретичними і фактичними частотами знаходиться розрахункове значення критерію Пірсона:

$$\chi^2_{\text{ñïîñò}} = \frac{\sum_{i=1}^{S}(N_i - N'_i)}{N'_i},$$

де N'_i – теоретичні частоти, N_i – емпіричні частоти.

Доведено, що при $S \to \infty$ закон розподілу будь-якої випадкової величини незалежно від того, якому закону розподілу підлягала генеральна сукупність, спрямований до закону розподілу χ^2 з $k = S-1$ ступенями свободи.

Із спеціальних таблиць в залежності від кількості ступенів свободи k та рівня значимості α знаходиться критичне значення критерію Пірсона $\chi^2_{\text{êðèò}}(\alpha;k)$. Якщо $\chi^2_{\text{ñïîñò}} < \chi^2_{\text{êðèò}}$ - немає підстав відкинути нульову гіпотезу, тобто теоретичний та емпіричний закони розподілу однорідні. У випадку, коли $\chi^2_{спост} < \chi^2_{крит}$, нульову гіпотезу відкидають (теоретичний та емпіричний закони розподілу не однорідні).

Тепер зупинимося на оцінці теоретичних частот закону розподілу. Звернемося до прикладу. Нехай є малюнок 24-розрядного формату BMP (рис. 1).

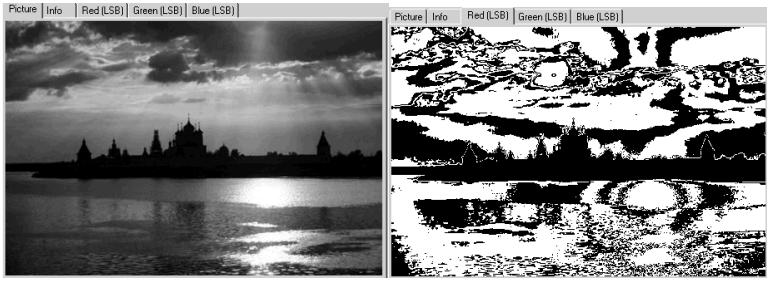

Рис.1. Червона компонента повнокольорового зображення та її найменш значущі біти

Для певного класу BMP-зображень найменш значущі біти не є шумовими. Якщо подивитись на малюнок, поданий на рис. 1, можна чітко бачити залежність між LSB та інтенсивністю кольору зображення пікселя. На малюнку наближену до мінімуму інтенсивність червоної кольорової компоненти має церква (майже чорна). Майже всі найменш значущі біти цієї

частини малюнку мають значення 0. Найяскравіше місце на малюнку – відбитки сонячних променів від поверхні річки. Тут значення кольорової компоненти наближається до максимального (майже всі найменш значущі біти цієї частини мають значення 1).

Коли ж в LSBs приховується інформація, наприклад, кодований текст, розподіл LSB буде наближатися до випадкового.

Нехай інформація приховується у частині зображення, яка має однаковий колір. Наприклад, майже весь чорний. Перед вбудовуванням повідомлення майже всі пікселі зображення будуть мати значення 0. Тому LSBs будуть мати нульові значення. Після вбудовування випадкового повідомлення, розподіл LSBs буде прямувати до співвідношення 50/50.

Розглянемо декілька бітів (значення) зображення. Для значень довжиною 2 біти можна сформувати дві пари, які відрізняються лише останнім бітом. Якщо останній біт у парі значень містить вбудовану інформацію, їх кількість для малюнка приблизно однакова. Пари значень довжиною 2 біти показані в табл. 1.

Таблиця 1

0**0** 0**1**	Перша пара значень.
1**0** 1**1**	Друга пара значень.

Для значень довжиною три біти можна сформувати 4 пари які відрізняються лише одним бітом. Ці пари значень показані в табл. 2.

Таблиця 2

00**0** 00**1**	Перша пара значень.
01**0** 01**1**	Друга пара значень.
10**0** 10**1**	Третя пара значень.
11**0** 11**1**	Четверта пара значень.

Аналогічно формуються пари значень довжиною у 8 біт (табл. 3).

Таблиця 3

0000 000**0** 0000 000**1**	Перша пара значень.
0000 001**0** 0000 001**1**	Друга пара значень.
...	...
1111 110**0** 1111 110**1**	127 пара значень.
1111 111**0** 1111 111**1**	128 пара значень.

Отже для кольорової компоненти, яка приймає 256 значень, формується 128 пар. Далі підраховуються частоти, з якими зустрічаються значення в парах і знаходиться середнє арифметичне для кожної пари значень. Одержані величини і є теоретичними частотами пар значень при наявності вбудованих даних.

Розглянемо працездатність цього методу стеганоаналізу на деяких стандартних стеганографічних програмах вбудовування даних.

Використовуючи програму ***EzStego***, вбудовуємо в малюнок, поданий на рис. 1, текстову інформацію, яка займає 45% від максимально можливої.

Діаграма на рис.2, одержана з використанням описаної методики вказує місцеположення вбудованої інформації у файлі зображення. Це підтверджується зображенням малюнок ліворуч на рис.2, де показано розподіл LSB зображення.

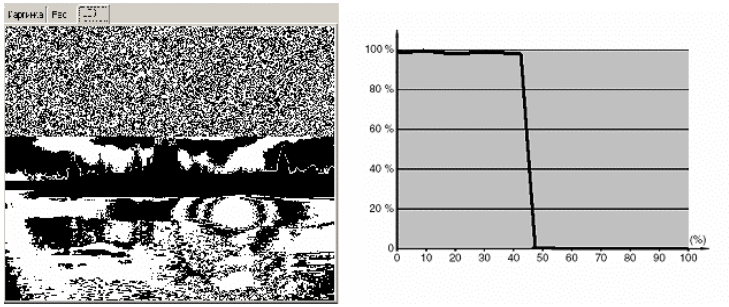

Рис.2 Найменш значущі біти малюнка із вбудованою інформацією та аналіз факту вірогідності вбудовування інформації

Варто зазначити, що описана методика не є універсальною. Вона спрацьовує лише для послідовного вкладення прихованої інформації, тобто вкладення у кожний послідовний байт зображення. Якщо використати, наприклад, програму ***S-Tools***, яка розподіляє вбудовані біти по всьому зображенню, а кількості інформації недостатньо для заповнення всіх байт зображення, то виявлення прихованих вкладень не відбувається.

Список літератури: *1. Генне О.В.* Стеганография: основные положения стеганографии //Конфидент № 3 (33) май - июнь 2000 г. *2. Westfeld A. and Pfitzmann A.* Attack on Steganographic Systems, Lectures Notes in Computer Science, vol. 1768, Springer-Verlag, Berlin, 2000, pp. 61-75 *3. Гурман В.Е.* Теория вероятностей и математическая статистика: Учебное пособие для ВУЗов. М.: Высш. шк., 2003. – 479 с.:

Надійшла до редколегії 05.04.07

УДК 519.146

В. П. ПУТЯТИН, д-р. техн. наук, зав. каф. кибернетики ХНТУСХ им. П. Василенко, ***А. Б. ЭЛЬКИН***, соискатель ХНТУСХ им. П.Василенко

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ЗАДАЧИ ОПТИМИЗАЦИИ РАЗБИЕНИЙ В АПК

Розглянуто математичну модель задачі оптимізації розбиття двовимірної області складної форми на підобласті рівної площі. Такі задачі виникають, наприклад, при передачі земельних наділів з колективної у особисту власність членів сільгосппідприємств. Досліджуються специфічні особливості математичної моделі, які у подальшому лягли в основу чисельної реалізації математичної моделі.

Рассмотрена математическая модель задачи оптимизации разбиения двумерной области сложной формы на подобласти равной площади. Такие задачи возникают, например, при передаче земельных наделов из коллективной в частную собственность членов сельхозпредприятий. Исследуются особенности математической модели, которые в дальнейшем легли в основу численной реализации математической модели.

The mathematical model of problem of optimization of fragmentation a two-dimensional region of the complex form on subregions of equal area is considered. Such problems appear, for instance, at the disposition allotment from collective property in the private property of members of agricultural enterprise. The particularities of mathematical models, which underlie of numerical implementation of the mathematical models, are researched.

Введение. Реформирование аграрного сектора Украины требует разработки соответствующих методов и средств, базирующихся на техническом, технологическом, юридическом, экономическом и нормативном обеспечении. При этом, одной из проблем реформирования является процесс паевания земли, суть которого заключается в передаче земельных участков